THE CENTER FOR
INTERNET SECURITY SM

Deploying and Verifying Checklists
The Keys to Widespread Adoption

Clint Kreitner
www.cisecurity.org
ckreitner@cisecurity.org

Better user understanding of what is causing the vulnerabilities that are being exploited

- Software defects
  - Fixed with vendor patches
- Lack of technical security controls
  - Security settings made to enable or disable security features of the OS software

Better user understanding of how high level standards tie with technical security settings

- ISO 17799
- COBIT from ISACA
- SysTrust, WebTrust from AICPA
- FISCAM from GAO
- Principles and Practices for Security of IT Systems from NIST
- Standard of Good Practice from ISF

The high level standards are helpful, but incomplete

- They describe “what” to do, but not “how”
- These standards are effective only when accompanied by details on how to implement their requirements

An Example from ISO 17799
9.7.1 Event logging

Audit logs recording exceptions and other security-relevant events should be produced and kept for an agreed period to assist in future investigations and access control monitoring.

Audit logs should also include:
a) user IDs;
b) dates and times for log-on and log-off;
c) terminal identity or location if possible;
d) records of successful and rejected system access attempts;
e) records of successful and rejected data and other resource access attempts.

One Way to Activate Event Logging on Sun Solaris Systems:

```
cat <<END_SCRIPT >/etc/init.d/newperf
#!/sbin/sh
/usr/bin/su sys -c
"/usr/lib/sa/sadc /var/adm/sa/sa`date +%d`"
END_SCRIPT
chown root:sys /etc/init.d/newperf
chmod 744 /etc/init.d/newperf
ln -f /etc/init.d/newperf
/etc/rc2.d/S21newperf
/usr/bin/su sys -c crontab <<END_ENTRIES
0,20,40 * * * * /usr/lib/sa/sa1
45 23 * * * /usr/lib/sa/sa2 -s 0:00 -e 23:59 -i 1200 -A
END_ENTRIES
```

Why has it been so difficult to proliferate good security practice?

- Vendors have been shipping systems to users with technical security controls turned off
- Users don't know how to properly configure their systems
- Users are afraid to disrupt operations
  - With patching or security settings

Why else would this be true?

Microsoft Issues Patches, But Users Don't Apply Them

	Attack date	Advance notice
SQL Slammer	1/25/03	185 days
Bugbear	9/30/02	502 days
Frethem	7/17/02	427 days
Yaha	6/22/02	402 days
ElKern	4/17/02	336 days
Klez	4/17/02	336 days
Badtrans	11/24/01	192 days
Nimda	9/18/01	336 days
Code Red	7/19/01	31 days
	Average: 305 days	

Source: McAfee, MessageLabs, Microsoft, Symantec, and Sophos

Forrester Research Report

April 3, 2003

More sharply targeted configuration recommendations

- Different security levels
- Different system roles

Different levels of hardening

- Levels of Security
  - Legacy – Level I
  - Enterprise – Level II
  - High – Level III (Gold Standard)

Different system roles

- Role-based security benchmarks
  - Domain member workstation
  - Domain member server
  - Domain Controller
  - Standalone workstation
  - Standalone server
  - Laptop
  - Bastion Server
  - IIS Server
  - File & Print Server

Benchmarks are needed for:

- Common OS/application combinations
  - Definitive verification of breakage via testing
- Appliances
  - Copiers, scanners, printers, etc.

The importance of broad consensus among security experts

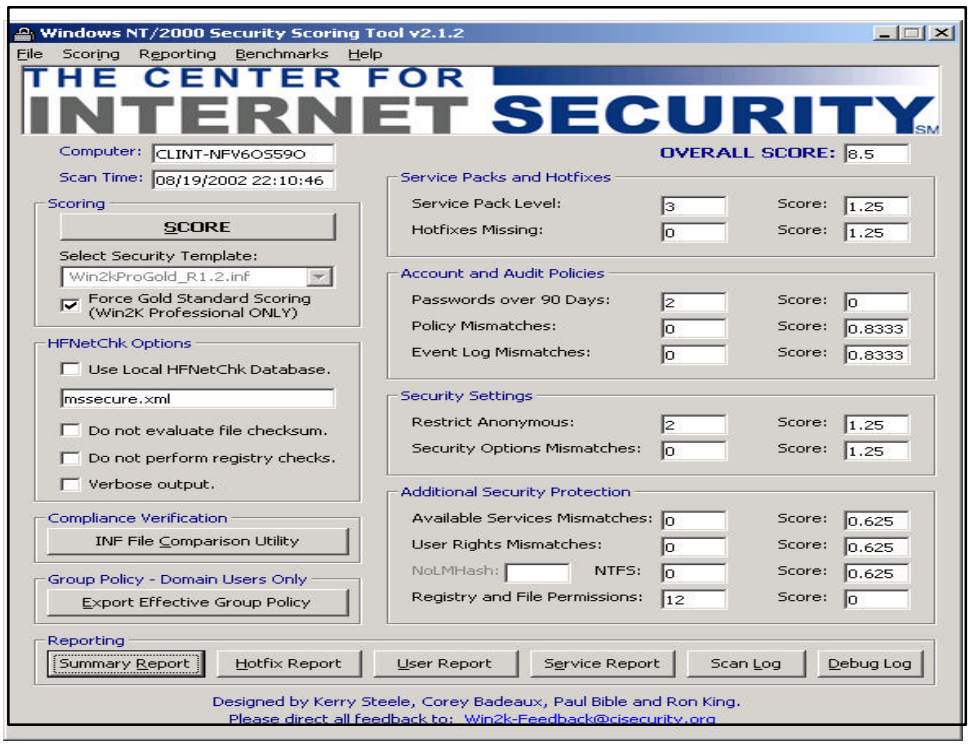
- There is such a thing as too many sources of guidance
  - How are users to choose from among those available?

The crucial role of scoring tools

- Motivate behavior toward more robust security
- Enable tracking of configuration status over time
- Helps communication between security specialists and managment

How about:

- Databases of scores by sector
  - Anyone here want to be on the left hand side of the distribution curve?
  - The CI model works well here



The value of case studies

- (1) Scan a system “out of the box” and list identified vulnerabilities
- (2) Configure the system with the appropriate benchmark
- (3) Rescan the system and note the vulnerabilities remaining

Vulnerability Assessment Case studies

Study	System	Benchmark	% of Vuls Eliminated
Solutionary	W2K Server	Level I	85
Citadel	W2K Pro	Level I	81
NSA	W2K Pro	Level II	91
Mitre	W2K Pro	Level II	83 (CVE)
Citadel	W2K Server	Level II	99
Citadel	RedHatLinux	Level I	100

Encouraging progress

- Federal gov't promulgation of CIS benchmarks and tools via FedCIRC
- VISA adoption of CIS benchmarks for its Cardholder Information Security Program's Digital Dozen
- Progress at the vendor level
  - Dell's decision to offer pre-configured W2K systems
  - Top security experts from Microsoft, Sun, HP, Cisco, and Oracle are active on the benchmark teams
  - AOL's decision to work with CIS on an AOL User's benchmark and easy to use implementation tools

Management benefits of using benchmarks and tools

- Substantially reduce the risk of unauthorized intrusion
- Following a recognized patching and configuration standard demonstrates due care against legal liability
- Provides a basis for ongoing measurement and reporting of security status to management
  - FISMA

What will foster better configuration and patching practices?

- Incorporation in procurement req'ts by government and corporate buyers
  - Vendors will ship safer systems
- Compliance required by corporate audits
- Agencies serious about compliance with FISMA req'ts
- Organizational desire to demonstrate due care against potential legal liability

What will foster better configuration and patching practices?

- Insurance premium discounts for demonstrated compliance
- ISP's getting in the game to make compliance with the "Big Four" easy for their customers
  - Anti-virus
  - Firewall
  - Up to date patching
  - Sound configuration practice

Thank you!

dl.ettner@cisecurity.org
http://www.cisecurity.org